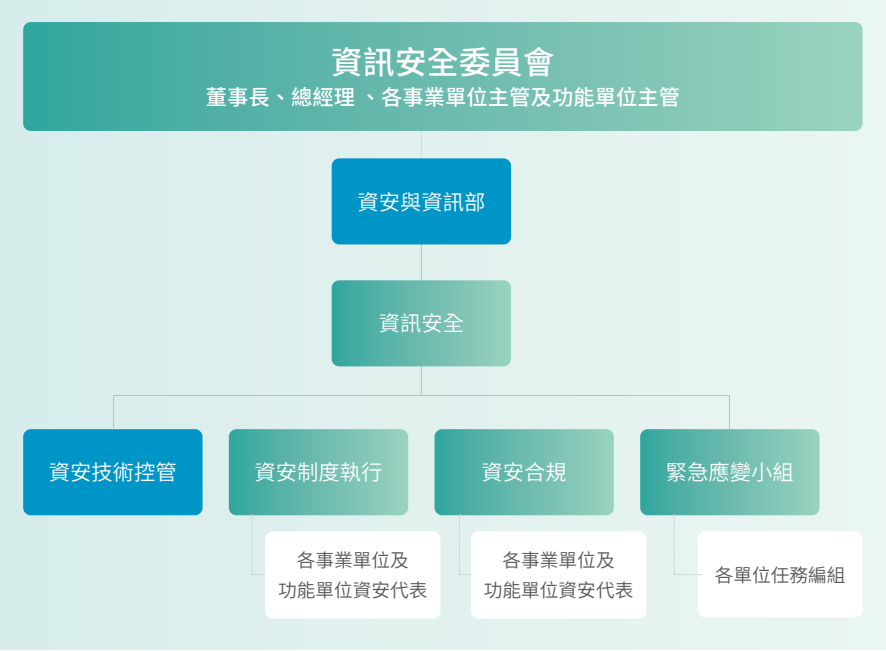
2.5 資訊安全與隱私權管理

光寶重視各利害關係人，包括內部員工、外部合作夥伴 (客戶、供應商與顧問等)、股東及營運相關資訊資產之安全與隱私，於 2018 年推動全公司資訊安全管理制度以依循 ISO 27001：2013 國際標準訂立光寶「資訊安全政策」，作為資訊安全管理依據，同時因應歐盟通用數據保護條例 (General Data Protection Regulation, GDPR) 法規之要求，確保個人資料之蒐集、處理或利用符合 GDPR 及台灣個人資料保護法等相關法規及主管機關之要求，於 2020 著手修訂個人資料保護安全政策（以下簡稱本政策）及相關管理辦法，作為個人資料保護工作之指導方針，落實於光寶全球據點，透過跨部門、跨功能資訊安全組織推動資訊安全相關工作。同時持續導入資訊科技管理工具及不斷強化資訊安全管理機制，以持續有效運作資訊安全管理及隱私權保護等機制。2020 年間並無侵犯客戶隱私或遺失客戶資料相關投訴事件發生。

資訊安全組織架構

於 2018 年成立跨部門、跨功能之資訊安全委員會，由董事長及總經理擔任委員會召集人，於 2020 年將資安部併入資訊部，並將資訊部更名為資安與資訊部，主要執行資訊安全防護相關工作、資訊安全事件應變處理及資訊安全事件事後復原能力，以預防資訊安全事件之發生及降低資訊安全事件之損失。



資訊安全管理及稽核機制

為落實資訊安全管理機制並確保資訊資產之機密性、完整性及可用性，光寶依循 ISO 27001：2013 國際標準制訂資訊安全管理文件，並以 PDCA 循環運作模式建立、實施、維護與改善資訊安全管理制度，於 2020 年取得 ISO 27001 資訊安全管理系統驗證；同時於 2020 年培訓資訊安全查核團隊，該團隊查核人員也個別取得 ISO 27001：2013 主導稽核員證照。

資訊安全技術控管建置

1. 透過建置資訊安全監控系統及執行系統弱點掃描以預防駭客侵入及竊取公司機密資料。建立完整資訊系統安全防護網，包含機房、網路設備、網路連線及個人資訊設備 (例如桌上型電腦、筆記型電腦、平板電腦及智慧型手機等) 管理，以落實員工個人資料、公司機密資料、客戶及供應商等資料保護。

2. 為確保光寶資料保護，導入微軟 Azure 資訊保護 (簡稱 AIP) 機制，運用雲端數位化工具，如微軟 Office 365，加密機制、身分識別、授權原則及遠端安全存取機制，以保護員工個人資料及企業機密文件。

資訊安全教育訓練

為提升光寶員工對資訊安全之意識與認知，於資訊安全管理文件訂立「人員資訊安全要求及教育訓練管理程序」，以作為管理依據。

1. 資訊安全認知宣導：為提高員工資訊安全意識，適時透過各種管道及會議進行資訊安全相關訊息公告及宣導。

2. 資訊安全教育訓練：
   (1) 新進員工報到當日即簽署從業人員職業道德服務協議並接受資訊安全相關教育訓練，以了解公司資訊安全政策與要求。
   (2) 每年執行員工常態性資訊安全教育訓練，所有同仁每年應至少參與資安教育訓練時數 1 小時。另針對不同角色與職能人員規劃不同性質資安課程，本年度已規劃至少 6 堂資安與隱私相關教育訓練課程，透過不斷的培訓以提升光寶員工資安意識並內化於各項作業中，以落實最安全及嚴密的資安保障。
   (3) 除光寶所舉辦之教育訓練外，資訊安全 (總) 資安代表及資訊安全查核人員須參與外部所舉辦之相關訓練活動或研討會，吸取資訊安全防護機制及最新資訊安全攻擊型態，以強化光寶資訊安全防護能量。
   (4) 每年透過不定期社交工程演練，強化員工資安意識提升。

資安控管機制	說明	資安風險控管
特權帳號控管	用戶端電腦本機管理員特權帳號管理系統	防範員工任意安裝非法盜版軟體或惡意軟體入侵
周邊裝置控管	用戶端電腦周邊裝置存取管控系統	防範員工藉可移動儲存裝置洩漏機敏資訊
上網存取控管	Internet 上網管控及威脅偵測系統	防範員工上惡意網站遭受病毒威脅入侵
資訊外洩控管	DLP(Data Lost Prevention) 用戶端電腦資料外洩防護	偵測機敏資訊外洩並記錄追蹤
資訊外洩控管	Conditional Access 使用公司電腦才可存取 O365 服務	防範機敏資訊外洩及駭客攻擊
系統弱點控管	電腦主機弱點偵測掃瞄系統	提供主機弱點檢查報告，防止威脅入侵
日誌稽核控管	主機日誌追蹤管理系統	提供資安事件稽查之相關軌跡日誌查詢
網路威脅控管	辦公室區域及工廠端網路異常流量及威脅偵測系統	防範網路勒索病毒擴散
手機存取管控	手持裝置 MAM/MDM/MTD 管控系統	防範員工使用個人手機裝置洩漏機敏資訊及威脅入侵
遠端存取管控	在公司外遠端連線管控系統	提供員工在公司外連到公司內部使用資訊應用系統